

1. (Currently Amended) A method, performed by a computer system, for collecting network usage data about users accessing a network and resources thereon without associating personally identifiable information with the usage data, comprising:

obtaining an identifier at a network service provider representing one or more users of a computer network;

creating an anonymized identifier using the identifier obtained from the network service provider;

collecting data being transmitted across the computer network at a collection engine connected to the network service provider;

associating the anonymized identifier with the collected data through the collection engine if the collected data is sent to or from the one or more users to create a transaction record; and

storing the transaction record by the collection engine in a database separate from the network service provider.

2. (Original) The method of claim 1, wherein the obtained identifier is a Mobile Subscriber Integrated Services Digital Network (MSISDN) number.

3. (Original) The method of claim 1, wherein the obtained identifier is a static Internet Protocol (IP) address.

4. (Original) The method of claim 1, wherein the anonymized identifier is created by applying a one-way hashing function to the obtained identifier.

5. (Original) The method of claim 1, wherein the anonymized identifier is created by applying a one-way hashing function to the obtained identifier and a security key.

6. (Original) The method of claim 5, wherein the one-way hashing function is the Secure Hashing Algorithm 1 (SHA-1).

7. (Original) The method of claim 5, wherein the one-way hashing function is the Message Digest 4 (MD4) algorithm.

8. (Original) The method of claim 5, wherein the one-way hashing function is the Message Digest 5 (MD5) algorithm.

9. (Original) The method of claim 5, wherein the one-way hashing function is the Digital Encryption Standard (DES).

10. (Previously Presented) The method of claim 1, wherein the act of obtaining an identifier representing one or more users of a computer network includes:

receiving packets at the network service provider sent by an authentication server; and
extracting an identifier at the network service provider from the received packets.

11. (Original) The method of claim 10, wherein the authentication server is a RADIUS authentication server.

12. (Original) The method of claim 11, wherein the received packets are RADIUS authentication packets.

13. (Original) The method of claim 10, wherein the authentication server is a Dynamic Host Configuration Protocol (DHCP) server.

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (New) The method of claim 1, wherein said collection engine is a passive device, and further comprising monitoring network traffic, collecting data about network transactions and recording the data in a database.

29. (New) The method of claim 28, further comprising creating online behavioral profiles unassociated with individual users, with the collection engine.

30. (New) The method of claim 28, wherein multiple collection engines monitor network traffic, collect data about network transactions and record the data in a database, and further

comprising, configuring and managing said multiple collection engines and aggregating data collected therewith through the use of an aggregation server.

31. (New) A method, performed by a computer system, for collecting network usage data about users accessing a network and resources thereon without associating personally identifiable information with the usage data, consisting substantially of:

- obtaining an identifier at a network service provider representing one or more users of a computer network;

- creating an anonymized identifier using the identifier obtained from the network service provider;

- collecting data being transmitted across the computer network at a collection engine connected to the network service provider;

- associating the anonymized identifier with the collected data through the collection engine if the collected data is sent to or from the one or more users to create a transaction record; and

- storing the transaction record by the collection engine in a database separate from the network service provider.